

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): OHYA, et al.
Serial No.: Not yet assigned
Filed: April 2, 2004
Title: INFORMATION MANAGEMENT METHOD
Group: Not yet assigned

LETTER CLAIMING RIGHT OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

April 2, 2004

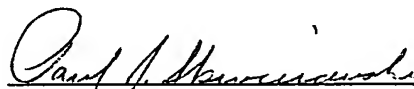
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2003-382589, filed November 12, 2003.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Paul J. Skwierawski
Registration No. 32,173

PJS/alb
Attachment
(703) 312-6600

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年11月12日
Date of Application:

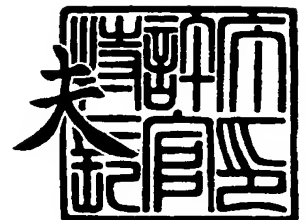
出願番号 特願2003-382589
Application Number:
[ST. 10/C]: [JP 2003-382589]

出願人 株式会社日立製作所
Applicant(s):

2004年 3月18日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2004-3022077

【書類名】 特許願
【整理番号】 340300924
【提出日】 平成15年11月12日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 17/60
【発明者】
 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報・通信グループ内
 【氏名】 大屋 徹治
【発明者】
 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報・通信グループ内
 【氏名】 一木 眞吾
【発明者】
 【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社日立製作所 エンタープライズサーバ事業部内
 【氏名】 西川 和幸
【発明者】
 【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社日立製作所 エンタープライズサーバ事業部内
 【氏名】 小林 実
【発明者】
 【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社日立製作所 エンタープライズサーバ事業部内
 【氏名】 大竹 伸一
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社日立製作所
【代理人】
 【識別番号】 110000176
 【氏名又は名称】 一色国際特許業務法人
 【代表者】 一色 健輔
【手数料の表示】
 【予納台帳番号】 211868
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

機密情報管理を支援する情報処理装置であって、

機密情報を含む管理対象ファイルを入力インターフェイスにて受け付けて、この管理対象ファイルより、ファイル ID、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出する管理マスタ抽出部と、

管理対象ファイル毎に前記管理マスタ情報が登録されたファイル管理データベースを格納する記憶装置と、

前記管理対象ファイルの前記記憶装置への格納事象を出力インターフェイスに出力する格納事象出力部と、

管理対象ファイルの消去リクエストを入力インターフェイスにて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル管理データベースにおいて抽出する消去対象抽出部と、

前記消去対象抽出部において抽出した管理対象ファイルの情報に基づき、前記記憶装置における該当管理対象ファイルの消去を実行するファイル消去部と、

前記ファイル消去部により消去された管理対象ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新する管理マスタ情報更新部と、

前記ファイル消去部により管理対象ファイルが消去された旨を、出力インターフェイスに出力する消去情報出力部と、

を備えることを特徴とする情報処理装置。

【請求項 2】

請求項 1 に記載の情報処理装置において、

前記消去リクエストに含まれる消去モード情報が、管理対象ファイルの消去に加えて管理マスタ情報の消去も要求するモードであった場合、前記ファイル管理データベースにおける該当管理対象ファイルの管理マスタ情報を特定し、消去する管理マスタ情報消去部と

を備えることを特徴とする情報処理装置。

【請求項 3】

請求項 1 に記載の情報処理装置において、

管理対象ファイルのバックアップリクエストを入力インターフェイスにて受け付けて、このバックアップリクエストに対応する管理対象ファイルのアクセス権限を、前記ファイル管理データベースにおいて抽出するアクセス権限抽出部と、

前記バックアップリクエストに対応するユーザのユーザ権限を入力インターフェイスにて受け付けて、このユーザ権限と前記アクセス権限とを照合し、前記バックアップリクエストに対応する管理対象ファイルのアクセス可否を判定するアクセス権限判定部と、

前記アクセス権限判定部においてアクセス可能たる判定がなされた場合、前記バックアップリクエストに対応する管理対象ファイルを前記記憶装置より抽出して、当該管理対象ファイルの複製ファイルを生成する複製生成部と、

前記管理対象ファイルの複製ファイルをバックアップ媒体に出力する複製出力部と、

前記複製ファイルの管理マスタ情報を抽出し、ファイル管理データベースに格納する複製ファイル登録部と、

を備えることを特徴とする情報処理装置。

【請求項 4】

請求項 1 に記載の情報処理装置において、

管理対象ファイルの利用リクエストを入力インターフェイスにて受け付けて、この利用リクエストに対応する管理対象ファイルのアクセス権限を、前記ファイル管理データベースにおいて抽出するアクセス権限抽出部と、

前記利用リクエストに対応するユーザのユーザ権限を入力インターフェイスにて受け付けて、このユーザ権限と前記アクセス権限とを照合し、前記利用リクエストに対応する管

理対象ファイルのアクセス可否を判定するアクセス権限判定部と、

前記アクセス権限判定部においてアクセス可能たる判定がなされた場合、前記利用リクエストに対応する管理対象ファイルを前記記憶装置より抽出して、出力インターフェイスに出力する利用ファイル出力部と、

前記利用ファイル出力部により出力された管理対象ファイルに対する更新処理を、入力インターフェイスより受け付けて、更新ファイルを生成する更新ファイル生成部と、

前記更新ファイルを前記記憶装置に格納する更新ファイル格納部と、

前記更新ファイルの管理マスタ情報を抽出し、ファイル管理データベースに格納する更新ファイル登録部と、

を備えることを特徴とする情報処理装置。

【請求項 5】

請求項 3 または 4 に記載の情報処理装置において、

前記消去リクエストに対応する管理対象ファイルの情報に加えて、当該管理対象ファイルから派生した複製ファイルまたは更新ファイルの情報を、前記ファイル管理データベースにおいて抽出する関連消去対象抽出部と、

前記関連消去対象抽出部により抽出された複製ファイルまたは更新ファイルの情報に基づき、前記記憶装置またはバックアップ媒体における該当ファイルの消去を実行する関連ファイル消去部と、

前記関連ファイル消去部により消去された複製ファイルまたは更新ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新する関連管理マスタ情報更新部と、

前記関連ファイル消去部により複製ファイルまたは更新ファイルが消去された旨を、出力インターフェイスを介して、当該情報処理装置とネットワークを介して接続された第 2 の情報処理装置に通知する通知部と、

を備えることを特徴とする情報処理装置。

【請求項 6】

請求項 1 に記載の情報処理装置において、

管理対象ファイルを利用する業務アプリケーションの実行に際し、管理対象ファイルの消去権限、バックアップ権限、および利用権限のいずれかの有無をユーザ毎に定めた業務処理権限データベースにおいて、該当ユーザの権限有無を判定する業務アプリケーション処理判定部と、

前記業務アプリケーション処理判定部において、管理対象ファイルの消去権限、バックアップ権限、および利用権限のいずれかの権限をユーザが有する判定がなされた場合、業務アプリケーションの処理対象となる管理対象ファイルを前記記憶装置より抽出して、業務アプリケーションに提供する業務アプリケーション処理実行部と、

を備えることを特徴とする情報処理装置。

【請求項 7】

請求項 1 または 5 に記載の情報処理装置において、

前記ファイル消去部または関連ファイル消去部により、前記記憶装置またはバックアップ媒体における管理対象ファイルまたは複製ファイル或いは更新ファイルの消去を実行した後、当該記憶装置またはバックアップ媒体の格納情報を、第 2 の記憶装置にコピーする第 1 コピー実行部と、

前記記憶装置またはバックアップ媒体におけるセクタなどの記憶単位毎に、所定パターンのデータを所定回書き込みする第 1 消磁実行部と、

前記第 2 の記憶装置の格納情報を、前記記憶装置またはバックアップ媒体にコピーする第 2 コピー実行部と、

前記第 2 の記憶装置におけるセクタなどの記憶単位毎に、所定パターンのデータを所定回書き込みする第 2 消磁実行部と、

を備えることを特徴とする情報処理装置。

【請求項 8】

機密情報の管理を情報処理装置により行う方法であって、
機密情報を含む管理対象ファイルを入力インターフェイスにて受け付けて、この管理対象ファイルより、ファイルID、当該管理対象ファイルへのアクセス権限、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出し、
管理対象ファイル毎の前記管理マスタ情報を、ファイル管理データベースに登録し、
前記管理マスタ情報と紐付けて管理対象ファイルを格納し、
前記管理対象ファイルの前記記憶装置への格納事象を出力インターフェイスに出力し、
管理対象ファイルの消去リクエストを入力インターフェイスにて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル管理データベースにおいて抽出し、
前記ファイル管理データベースにおいて抽出した、消去リクエストに対応する管理対象ファイルの情報に基づき、前記記憶装置における該当管理対象ファイルの消去を実行し、
前記記憶装置において消去された該当管理対象ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新し、
前記管理対象ファイルが消去された旨を、出力インターフェイスに出力することを特徴とする機密情報管理方法。

【請求項 9】

機密情報の管理方法を情報処理装置に実行させるためのプログラムであって、
機密情報を含む管理対象ファイルを入力インターフェイスにて受け付けて、この管理対象ファイルより、ファイルID、当該管理対象ファイルへのアクセス権限、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出するステップと、
管理対象ファイル毎の前記管理マスタ情報を、ファイル管理データベースに登録するステップと、
前記管理マスタ情報と紐付けて管理対象ファイルを格納するステップと、
前記管理対象ファイルの前記記憶装置への格納事象を出力インターフェイスに出力するステップと、
管理対象ファイルの消去リクエストを入力インターフェイスにて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル管理データベースにおいて抽出するステップと、
前記ファイル管理データベースにおいて抽出した、消去リクエストに対応する管理対象ファイルの情報に基づき、前記記憶装置における該当管理対象ファイルの消去を実行するステップと、
前記記憶装置において消去された該当管理対象ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新するステップと、
前記管理対象ファイルが消去された旨を、出力インターフェイスに出力するステップと、
を含むことを特徴とする機密情報管理プログラム。

【請求項 10】

請求項 9 に記載の機密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【書類名】明細書

【発明の名称】 情報管理を支援する情報処理装置、情報管理方法、プログラム、および記録媒体

【技術分野】**【0001】**

本発明は、個人もしくは企業などの組織の情報処理装置に記録された機密情報を含む消去対象となる情報を管理する技術に関する。その中でも特に、いわゆるアウトソーシングと呼ばれる業務（処理）委託で受託側の使用した情報の消去を実行するための技術に関する。なお、本発明の機密情報には、いわゆる個人情報、機密情報が含まれる。

【背景技術】**【0002】**

業務効率の向上を目的に、業務のアウトソーシングを行う企業が増えている。一方で、個人情報や機密情報の保護確立の必要性も叫ばれている。そこで、このような個人情報や機密情報の適正な利用後には、これら情報が格納されたハードディスクなどの記憶装置において、全情報を消去する手法などが提案されている。

【0003】

例えば、情報の記録された磁気ディスクを破棄する際、容易でしかも瞬時にその情報を消去でき、安定した効果を発揮して磁気ディスクの情報を完全に消去できる方法およびその装置を提供するとの目的の下、ハードディスクの磁気ディスクのディスク面と水平方向に直流磁界を印加して磁気配列を一方向に整列させて情報を消去する方法において、磁気ディスクに対し水平方向の直流磁界と同一方向へ前記磁気ディスクを移動させて情報を消去する磁気ディスクの情報消去方法（特許文献1参照）などが提案されている。

【特許文献1】 特開2002-163801号公報

【発明の開示】**【発明が解決しようとする課題】****【0004】**

しかしながら、従来技術においては、業務や処理委託されている場合、受託側に残った情報を消去することに関しては、何ら考慮されていない。

【0005】

通常、業務もしくは処理委託が行われる場合、委託側から受託側へ情報が受け渡される。なお、この受け渡しは、ネットワークを介した送信、記憶媒体を運送することによる受け渡し、もしくは紙などに記載された情報を受託側のシステムに入力することが含まれる。そして、この受け渡された情報を用いて、受託側のシステムでは、委託側の要望に沿った処理が実行される。ここで、委託側と受託側の契約が終了するなどして受託側での処理の必要性がなくなった場合、受託側のシステムに情報が残ってしまう。この情報は、委託側にとって営業上の機密情報、個人情報などできるだけ第三者に知られたくない情報、つまり、必要がない場合、消去したい情報である。

【0006】

しかし、従来技術においては、単に情報を消去することしか記載されておらず、処理を委託した場合に、受託側に残る情報を、効率よく消去することに関しては、開示されていない。特に、受託側のシステムにおいて、複数の委託者の情報のうち、契約の終了等があった委託者の情報を消去することに関しては、何ら開示されていない。このことは、従来提案されてきた情報消去の手法が以下の通りであることからわかる。

【0007】

従来提案されてきた情報消去の手法は、たとえばハードディスクなどの記憶装置の全セクタにわたって「0」または「1」などの所定パターンのデータを3回以上といった所定回数書き込む、いわゆる「ホワイトニング」の手法が主たるものであった。このような手法では、ハードディスクなどの記憶装置内における全データが消去されるものの、特定のファイルだけについて完全消去するといった技術は提案されてこなかった。そうすると勿論、アウトソーシング等の業務中に取得される個人情報や機密情報のバックアップファイ

ルについて、その完全な消去方法などが考慮されることもなかった。

【0008】

他方、従来の文書管理システム等における、文書ファイル作成や更新といった情報の使用という観点での情報管理手法は既に存在する。しかしながら、ハードディスクなどの記憶装置における例えば物理レベルでの情報消去などは考慮されておらず、データの復元アプリケーションなどを用いることで、一旦消去したはずの情報を容易に復元されることとなっていた。

【0009】

そこで本発明は上記課題を鑑みてなされたものであり、任意の情報の管理を効率よく実現する情報管理を支援する情報処理装置、情報管理方法、プログラム、および記録媒体を提供することを主たる目的とする。

【課題を解決するための手段】

【0010】

上記課題を解決する本発明の情報処理装置は、機密情報管理を支援する情報処理装置であって、機密情報を含む管理対象ファイルを入力インターフェイスにて受け付けて、この管理対象ファイルより、ファイルID、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出する管理マスタ抽出部と、管理対象ファイル毎に前記管理マスタ情報が登録されたファイル管理データベースを格納する記憶装置と、前記管理対象ファイルの前記記憶装置への格納事象を出力インターフェイスに出力する格納事象出力部と、管理対象ファイルの消去リクエストを入力インターフェイスにて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル管理データベースにおいて抽出する消去対象抽出部と、前記消去対象抽出部において抽出した管理対象ファイルの情報に基づき、前記記憶装置における該当管理対象ファイルの消去を実行するファイル消去部と、前記ファイル消去部により消去された管理対象ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新する管理マスタ情報更新部と、前記ファイル消去部により管理対象ファイルが消去された旨を、出力インターフェイスに出力する消去情報出力部と、を備えることを特徴とする。

【0011】

また、機密情報の管理を情報処理装置により行う方法であって、機密情報を含む管理対象ファイルを入力インターフェイスにて受け付けて、この管理対象ファイルより、ファイルID、当該管理対象ファイルへのアクセス権限、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出し、管理対象ファイル毎の前記管理マスタ情報を、ファイル管理データベースに登録し、前記管理マスタ情報と紐付けて管理対象ファイルを格納し、前記管理対象ファイルの前記記憶装置への格納事象を出力インターフェイスに出力し、管理対象ファイルの消去リクエストを入力インターフェイスにて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル管理データベースにおいて抽出し、前記ファイル管理データベースにおいて抽出した、消去リクエストに対応する管理対象ファイルの情報に基づき、前記記憶装置における該当管理対象ファイルの消去を実行し、前記記憶装置において消去された該当管理対象ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新し、前記管理対象ファイルが消去された旨を、出力インターフェイスに出力することを特徴とする機密情報管理方法にかかる。

【0012】

また、機密情報の管理方法を情報処理装置に実行させるためのプログラムであって、機密情報を含む管理対象ファイルを入力インターフェイスにて受け付けて、この管理対象ファイルより、ファイルID、当該管理対象ファイルへのアクセス権限、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出するステップと、管理対象ファイル毎の前記管理マスタ情報を、ファイル管理データベースに登録するステップと、前記管理マスタ情報と紐付けて管理対象ファイルを格納するステップと、前記管理対象ファイルの前記記憶装置への格納事象を出力インターフェイスに出力するステップと、管理対象フ

ファイルの消去リクエストを入力インターフェイスにて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル管理データベースにおいて抽出するステップと、前記ファイル管理データベースにおいて抽出した、消去リクエストに対応する管理対象ファイルの情報に基づき、前記記憶装置における該当管理対象ファイルの消去を実行するステップと、前記記憶装置において消去された該当管理対象ファイルの、前記ファイル管理データベースにおける該当管理マスタ情報の有効性の情報を、無効の旨に更新するステップと、前記管理対象ファイルが消去された旨を、出力インターフェイスに出力するステップと、を含むことを特徴とする機密情報管理プログラムにかかる。このプログラムは、前記各ステップの動作を行うためのコードから構成されている。

【0013】

更に、機密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体にかかる。

【0014】

その他、本願が開示する課題、及びその解決方法は、発明の実施の形態の欄、及び図面により明らかにされる。

【発明の効果】**【0015】**

本発明によれば、任意の情報の管理を効率よく実現することが可能となる。

【発明を実施するための最良の形態】**【0016】**

以下に本発明の実施形態について図面を用いて詳細に説明する。図1は本実施形態における情報処理装置100を含むネットワーク構成図である。本実施形態における情報処理装置たる管理サーバ100（以下、サーバ100）は、本発明の情報処理装置の有する機能を実現するプログラム106をメモリ107に格納し、演算装置たるCPU108により読み出して実行する。なお、プログラム106、ファイル情報管理マスタ110、業務処理権限111は、通常HDD115に格納されており、処理を実行する場合、メモリ107に展開される。

【0017】

また、メモリ107にはファイル情報管理マスタデータベース110が格納されており、機密情報管理の管理対象たるファイルの属性情報をここで管理する。さらに、管理対象ファイルを利用する業務アプリケーションの実行時における、管理対象ファイルの消去権限、バックアップ権限、および利用権限のいずれかの有無をユーザ毎に定めた業務処理権限データベース111も格納されている。

【0018】

他に、情報処理装置100がLANやインターネット等のネットワーク120を介して外部装置と接続してデータ授受を実行したり、データ入出力を行う入出力インターフェイス109を備えている。さらに、管理対象ファイルを格納するハードディスク115や、管理対象ファイルの複製データを格納するバックアップ媒体116、さらに、管理対象ファイルやこれから派生した複製ファイルや更新ファイル等の消去処理に用いる第2の記憶装置117も備えるものとする。

【0019】

なお、前記バックアップ媒体116としては、電氣的、磁氣的、光学的を問わず情報を記録できればよく、磁気テープ、光ディスク、光磁気ディスク、フレキシブルディスク、およびハードディスクなどが想定できる。また、前記第2の記憶装置117としては例えばハードディスクが想定できる。

【0020】

また、前記プログラム106は、以下のようなブロックから構成される。すなわち、機密情報を含む管理対象ファイルを入出力インターフェイス109（入力インターフェイス）にて受け付けて、この管理対象ファイルより、ファイルID、および当該管理対象ファイルの有効性の情報を含む管理マスタ情報を抽出する管理マスタ抽出部10を含むのもで

ある。なお、管理対象ファイル毎の前記管理マスタ情報を、ファイル情報管理マスタデータベース 110（ファイル管理データベース）に登録する管理マスタ登録部 11 を含むこともできる。

【0021】

さらに、前記管理対象ファイルの前記ハードディスク 115（記憶装置）への格納事象を入出力インターフェイス 109（出力インターフェイス）に出力する格納事象出力部 12 と、管理対象ファイルの消去リクエストを入出力インターフェイス 109（入力インターフェイス）にて受け付けて、この消去リクエストに対応する管理対象ファイルの情報を、前記ファイル情報管理マスタデータベース 110 において抽出する消去対象抽出部 13 と、を含むものである。

【0022】

また、前記消去対象抽出部 13 において抽出した管理対象ファイルの情報に基づき、前記ハードディスク 115 における該当管理対象ファイルの消去を実行するファイル消去部 14 と、このファイル消去部 14 により消去された管理対象ファイルの、前記ファイル情報管理マスタデータベース 110 における該当管理マスタ情報の有効性の情報を、無効の旨に更新する管理マスタ情報更新部 15 と、前記ファイル消去部 14 により管理対象ファイルが消去された旨を、入出力インターフェイス 109（出力インターフェイス）に出力する消去情報出力部 16 と、を含むものである。

【0023】

さらに、前記消去リクエストに含まれる消去モード情報が、管理対象ファイルの消去に加えて管理マスタ情報の消去も要求するモードであった場合、前記ファイル情報管理マスタデータベース 110 における該当管理対象ファイルの管理マスタ情報を特定し、消去する管理マスタ情報消去部 18 と、を含むものである。

【0024】

また、管理対象ファイルのバックアップリクエストを入出力インターフェイス 109（入力インターフェイス）にて受け付けて、このバックアップリクエストに対応する管理対象ファイルのアクセス権限を、前記ファイル情報管理マスタデータベース 110 において抽出するアクセス権限抽出部 19 と、前記バックアップリクエストに対応するユーザのユーザ権限を入出力インターフェイス 109（入力インターフェイス）にて受け付けて、このユーザ権限と前記アクセス権限とを照合し、前記バックアップリクエストに対応する管理対象ファイルのアクセス可否を判定するアクセス権限判定部 20 と、を含むものである。

【0025】

さらに、前記アクセス権限判定部 20 においてアクセス可能たる判定がなされた場合、前記バックアップリクエストに対応する管理対象ファイルを前記ハードディスク 115 より抽出して、当該管理対象ファイルの複製ファイルを生成する複製生成部 21 と、前記管理対象ファイルの複製ファイルをバックアップ媒体 116 に出力する複製出力部 22 と、前記複製ファイルの管理マスタ情報を抽出し、ファイル情報管理マスタデータベース 110 に格納する複製ファイル登録部 23 と、を含むものである。

【0026】

また、管理対象ファイルの利用リクエストを入出力インターフェイス 109（入力インターフェイス）にて受け付けて、この利用リクエストに対応する管理対象ファイルのアクセス権限を、前記ファイル情報管理マスタデータベース 110 において抽出するアクセス権限抽出部 24 と、前記利用リクエストに対応するユーザのユーザ権限を入出力インターフェイス 109（入力インターフェイス）にて受け付けて、このユーザ権限と前記アクセス権限とを照合し、前記利用リクエストに対応する管理対象ファイルのアクセス可否を判定するアクセス権限判定部 25 と、を含むものである。

【0027】

さらに、前記アクセス権限判定部 25 においてアクセス可能たる判定がなされた場合、前記利用リクエストに対応する管理対象ファイルを前記ハードディスク 115 より抽出し

て、入出力インターフェイス 109（出力インターフェイス）に出力する利用ファイル出力部 26 と、前記利用ファイル出力部 26 により出力された管理対象ファイルに対する更新処理を、入出力インターフェイス 109（入力インターフェイス）より受け付けて、更新ファイルを生成する更新ファイル生成部 27 と、を含むものである。

【0028】

また、前記更新ファイルを前記ハードディスク 115 に格納する更新ファイル格納部 28 と、前記更新ファイルの管理マスタ情報を抽出し、ファイル情報管理マスタデータベース 110 に格納する更新ファイル登録部 29 と、を含むものである。

【0029】

さらに、前記消去リクエストに対応する管理対象ファイルの情報に加えて、当該管理対象ファイルから派生した複製ファイルまたは更新ファイルの情報を、前記ファイル情報管理マスタデータベース 110 において抽出する関連消去対象抽出部 30 と、この関連消去対象抽出部 30 により抽出された複製ファイルまたは更新ファイルの情報に基づき、前記ハードディスク 115 またはバックアップ媒体 116 における該当ファイルの消去を実行する関連ファイル消去部 31 と、を含むものである。

【0030】

また、前記関連ファイル消去部 31 により消去された複製ファイルまたは更新ファイルの、前記ファイル情報管理マスタデータベース 110 における該当管理マスタ情報の有効性の情報を、無効の旨に更新する関連管理マスタ情報更新部 32 と、前記関連ファイル消去部 31 により複製ファイルまたは更新ファイルが消去された旨を、入出力インターフェイス 109（出力インターフェイス）を介して、当該情報処理装置とネットワークを介して接続された第 2 の情報処理装置に通知する通知部 33 と、を含むものである。

【0031】

さらに、管理対象ファイルを利用する業務アプリケーションの実行に際し、管理対象ファイルの消去権限、バックアップ権限、および利用権限のいずれかの有無をユーザ毎に定めた業務処理権限データベース 111 において、該当ユーザの権限有無を判定する業務アプリケーション処理判定部 34 と、この業務アプリケーション処理判定部 34 において、管理対象ファイルの消去権限、バックアップ権限、および利用権限のいずれかの権限をユーザが有する判定がなされた場合、業務アプリケーションの処理対象となる管理対象ファイルを前記ハードディスク 115 より抽出して、業務アプリケーションに提供する業務アプリケーション処理実行部 35 と、を含むものである。

【0032】

また、前記ファイル消去部 14 または関連ファイル消去部 31 により、前記ハードディスク 115 またはバックアップ媒体 116 における管理対象ファイルまたは複製ファイル或いは更新ファイルの消去を実行した後、当該ハードディスク 115 またはバックアップ媒体 116 の格納情報を、第 2 の記憶装置 117 にコピーする第 1 コピー実行部 36 と、前記ハードディスク 115 またはバックアップ媒体 116 におけるセクタなどの記憶単位毎に、所定パターンのデータを所定回書き込みする第 1 消磁実行部 37 と、を含むものである。

【0033】

さらに、前記第 2 の記憶装置 117 の格納情報を、前記ハードディスク 115 またはバックアップ媒体 116 にコピーする第 2 コピー実行部 38 と、前記第 2 の記憶装置 117 におけるセクタなどの記憶単位毎に、所定パターンのデータを所定回書き込みする第 2 消磁実行部 39 と、を含むものである。

【0034】

続いて、前記ファイル情報管理マスタデータベース 110 および受託情報管理マスタデータベース 136 についてそのデータ構造を説明しておく。図 2 は本実施形態における、（a）ファイル情報管理マスタデータベースのデータ構造例、（b）受託情報管理マスタデータベースのデータ構造例を示す図である。

【0035】

前記ファイル情報管理マスタデータベース 1 1 0 は、管理対象ファイルのファイル ID をキーとして、ファイル名、登録時サイズ、現在サイズ、最終サイズ、アクセス権、ファイル状況、（ファイルの）作成者、最終更新者、ファイル有効期限（例：管理対象ファイルの委託元から予め設定されるもの）、登録日時、最終更新日時、派生元ファイル ID （例：このファイルが管理対象ファイルから複製或いは更新したファイルであった場合の、管理対象ファイルを指す）、登録時レポートファイル名（例：このファイル情報管理マスタデータベースに当該ファイルが登録された際に前記委託元へ通知される登録レポートの名称）、消去レポートファイル名（例：このファイル情報管理マスタデータベースあるいはハードディスクから当該ファイルが消去された際に前記委託元へ通知される消去レポートの名称）といった情報が関連づけされたレコードから構成されている。

【 0 0 3 6 】

また、受託情報管理マスタデータベース 1 3 6 は、受託者端末 1 3 5 に備えられるデータベースである。なお、受託者端末 1 3 5 は、例えば委託元から業務依頼を受けて、当該委託業務毎に管理対象ファイルを統括管理する受託者が備えるものである。またこのような端末のほかにも、サーバ 1 0 0 を含むシステムの管理を行うシステム管理者の端末 1 3 7 や、前記委託業務に応じた業務処理を実行する受託者側担当者が備える、利用者端末 1 3 8 などがネットワーク 1 2 0 を介してサーバ 1 0 0 と接続される。

【 0 0 3 7 】

前記受託情報管理マスタデータベース 1 3 6 は、例えば前記受託者端末 1 3 5 が受けた委託業務毎に設定された業務 ID をキーとして、業務名、使用ファイル ID （管理対象ファイルのファイル ID で、通常は複数登録されている）、使用範囲条件（管理対象ファイルにおける使用許可範囲）、アクセス権、契約状況、作成者、作成日時、契約最終更新日時（例：委託業務の契約に関するもの）、最終更新者、派生元業務 ID、管理ファイル状況といった情報が関連づけされたレコードから構成されている。

【 0 0 3 8 】

なお、前記サーバ 1 0 0 は、受託者端末 1 3 5、システム管理者端末 1 3 7、利用者端末 1 3 8 らをネットワーク 1 2 0 を介して利用する形態例の他、1 つの装置内に一体に、或いはいくつかの端末を組み合わせるといった例も想定できる。この場合、サーバ 1 0 0 は情報処理装置として受託者端末 1 3 5 や利用者端末 1 3 8 の機能をあわせて備えることとなる。また、前記ファイル情報管理マスタデータベース 1 1 0、業務処理権限データベース 1 1 1、受託情報管理マスタデータベース 1 3 6 らについても、ネットワーク 1 2 0 上の別々の装置におおの配置され、サーバ 1 0 0 の利用を受けるとする例だけでなく、一つの記憶装置において一体に備わっている例を想定することもできる。

【 0 0 3 9 】

更に、サーバ 1 0 0 と、受託者端末 1 3 5、システム管理者端末 1 3 7、利用者端末 1 3 8 らをつなぐネットワーク 1 2 0 に関しては、LAN やインターネットの他、専用回線や WAN（Wide Area Network）、電灯線ネットワーク、無線ネットワーク、公衆回線網、携帯電話網など様々なネットワークを採用することも出来る。また、VPN など仮想専用ネットワーク技術を用いれば、インターネットを採用した際にセキュリティ性を高めた通信が確立され好適である。

【 0 0 4 0 】

次に、本発明の機密情報管理方法が適用されるビジネスモデル例について説明しておく。本実施形態に適用できるビジネスモデルとして図 3 に示す形態があげられる。ここでは、例えばある業務を委託する委託側と、この委託側から業務を受託する受託側の存在が想定できる。

【 0 0 4 1 】

委託側では、例えば業務委託 N を受託側に依頼するものとする。この業務委託 N は、受託側の受託者端末 1 3 5 を介してサーバ 1 0 0 に格納される電子ファイル 3 0 0 である。また、この電子ファイル 3 0 0 は、依頼要件を記述した要件書 3 0 1 と、個人情報などの機密情報が含まれる管理対象ファイル 3 0 2 とからなる。例えば前記業務委託 N の内容が

、顧客リストに従って販売促進用の電子メールを配信するものだとすれば、前記管理対象ファイル302にはメール送信先の情報を含む顧客リストが含まれることとなる。つまりは、この顧客リスト等が、本発明の機密情報管理方法における管理対象となる。

【0042】

サーバ100では、前記電子ファイル300の登録を受託者端末135より受け付けて、前記ハードディスク115に格納する一方で、ファイル情報管理マスタデータベース110において顧客リストを管理対象ファイル302として登録している（管理サーバ：状態1）。この例での受託側は、この業務Nの他にも、業務Aおよび業務iを受託している。

【0043】

他方、前記業務委託Nに対応する業務Nの担当者は、利用者端末138をもってサーバ100における前記顧客リストの情報を活用し、受託した業務を遂行する。なお、前記管理対象ファイル302は、受託業務毎に受託者端末135において管理される。

【0044】

また、例えば前記業務Nが完了するか、或いは契約が終了した場合などは、業務報告書350が委託側に送信される（サーバ100または受託者端末135が実行）。この業務報告書350は、電子的なものであっても、紙に出力されたものであってもよい。電子的なものである場合、ネットワークを介して受託側のシステムに送信する。また、ファクシミリを利用して送信してもよい。さらに、前記管理対象ファイル302としての顧客リストの電子ファイルを、前記ハードディスク115から完全に消去する（管理サーバ：状態2）。このように管理対象ファイル302を消去した旨は、例えば消去完了報告書360として委託側に送信する。

【0045】

以下、本実施形態の機密情報管理方法の実際手順について説明する。なお、以下で説明する機密情報管理方法に対応する各種動作は、情報処理装置たるサーバ100のメモリ107が備えるプログラム106によって実現される。そして、このプログラム106は、以下に説明される各種の動作を行うためのコードから構成されている。図4は本実施形態の機密情報管理方法におけるファイル登録手順を示すフロー図である。

【0046】

前記サーバ100は、受託者端末135における登録希望の管理対象ファイル選択（s1000）を受けて、これを受信する。さらに、受信した管理対象ファイルより、ファイルID、当該管理対象ファイルへのアクセス権限、および当該管理対象ファイルの有効性の情報を少なくとも含む管理マスタ情報を抽出し、ファイル情報管理マスタデータベース110に登録する（s1001）。また、前記管理対象ファイルは、例えば所定の暗号化手法（暗号鍵など）を用いて暗号化し、ハードディスク115に格納する（s1003）。

【0047】

前記管理対象ファイルの前記ハードディスク115への格納事象は、前記受託者端末135に通知される（s1004）。受託者端末135では、この通知をディスプレイなどの出力インターフェイスに出力表示する（s1005）。また、この通知に基づき、前記管理対象ファイルの登録情報を受託情報管理マスタデータベース136に登録する（s1006）。前記通知については、例えば管理対象ファイルの保存が完了したとの保存完了情報として印刷する（s1007）。このようにして、委託側から受託者端末135が受けた管理対象ファイルのサーバ100への登録が行われるのである。

【0048】

また、サーバ100に登録されている管理対象ファイルの閲覧利用が利用者端末138から行われる場合がある。図5は本実施形態の機密情報管理方法におけるファイル閲覧手順を示すフロー図である。このとき、利用者端末138では、閲覧希望の管理対象ファイルの選択（s1010）とその選択事象を含む利用リクエストの送信（s1011）がサーバ100に対して行われる。

【0049】

サーバ100ではこれを受け付けて、この利用リクエストに対応する管理対象ファイルの情報をファイル情報管理マスタデータベース110より抽出する(s1012)。このとき抽出する情報には、当該管理対象ファイルに関連づけられたアクセス権限の情報が含まれるものとする。他方で、ユーザ権限のチェック指示を利用者端末138に返す(s1013)。利用者端末138では権限チェック(s1015)を実行し、この結果をサーバ100に返信する(s1016)。なお、前記利用リクエストに対応するユーザのユーザ権限を利用者端末138より受け付けて、このユーザ権限と前記アクセス権限とをサーバ100が照合し、前記利用リクエストに対応する管理対象ファイルのアクセス可否を判定するとしてもよい。

【0050】

サーバ100では、前記チェック結果を受けて、ユーザ権限が前記アクセス権限にマッチするものでなければ(s1017：N)、権限エラーを利用者端末138側に出力する(s1018)。一方、ユーザ権限が前記アクセス権限にマッチするものであれば(s1017：Y)、前記利用リクエストに対応する管理対象ファイルを前記ハードディスク115より抽出する(s1019)。そしてこれを復号化して(s1020)、利用者端末138に送信する(s1021)。利用者端末138ではこれを受信して表示する(s1022)。

【0051】

図6は本実施形態の機密情報管理方法におけるファイルバックアップ手順を示すフロー図である。また、サーバ100に登録されている管理対象ファイルのバックアップ処理を実行する場合がある。このとき、例えば管理者端末138では、バックアップ希望の管理対象ファイルの選択(s1030)とその選択事象を含むバックアップリクエストの送信(s1031)がサーバ100に対して行われる。

【0052】

サーバ100ではこれを受け付けて、このバックアップリクエストに対応する管理対象ファイルの情報をファイル情報管理マスタデータベース110より抽出する(s1032)。このとき抽出する情報には、当該管理対象ファイルに関連づけられたアクセス権限の情報が含まれるものとする。他方で、ユーザ権限のチェック指示を管理者端末137に返す(s1033)。管理者端末137では権限チェック(s1035)を実行し、この結果をサーバ100に返信する(s1036)。なお、前記バックアップリクエストに対応する管理者のユーザ権限を管理者端末137より受け付けて、このユーザ権限と前記アクセス権限とをサーバ100が照合し、前記バックアップリクエストに対応する管理対象ファイルのバックアップ可否(アクセス可否)を判定するとしてもよい。

【0053】

サーバ100では、前記チェック結果を受けて、ユーザ権限が前記アクセス権限にマッチするものでなければ(s1037：N)、権限エラーを管理者端末137側に出力する(s1038)。一方、ユーザ権限が前記アクセス権限にマッチするものであれば(s1037：Y)、前記バックアップリクエストに対応する管理対象ファイルを前記ハードディスク115より抽出し(s1039)、これを復号化する(s1040)。さらに、当該管理対象ファイルの複製ファイルを生成し(s1041)、この複製ファイルをバックアップ媒体116に出力するのである。

【0054】

サーバ100は、続いて前記複製ファイルの管理マスタ情報を抽出し、ファイル情報管理マスタデータベース110において該当ファイルの更新処理を行う(s1042)。バックアップ処理が完了した旨は、管理者端末137に送信する(s1043)。管理者端末137ではこれを受信して表示する(s1044)。

【0055】

図7は本実施形態の機密情報管理方法におけるファイル更新手順を示すフロー図である。このとき、利用者端末138では、更新(或いは上書き、追加も含む)希望の管理対象

ファイルの選択 (s 1050) とその選択事象を含む更新リクエストの送信 (s 1051) がサーバ100に対して行われる。

【0056】

サーバ100ではこれを受け付けて、この更新リクエストに対応する管理対象ファイルの情報をファイル情報管理マスタデータベース110より抽出する (s 1052)。このとき抽出する情報には、当該管理対象ファイルに関連づけられたアクセス権限の情報が含まれるものとする。他方で、ユーザ権限のチェック指示を利用者端末138に返す (s 1053)。利用者端末138では、権限チェック (s 1055) を実行し、この結果をサーバ100に返信する (s 1056)。なお、前記利用リクエストに対応するユーザのユーザ権限を利用者端末138より受け付けて、このユーザ権限と前記アクセス権限とをサーバ100が照合し、前記利用リクエストに対応する管理対象ファイルのアクセス可否を判定するとしてもよい。

【0057】

サーバ100では、前記チェック結果を受けて、ユーザ権限が前記アクセス権限にマッチするものでなければ (s 1057: N)、権限エラーを利用者端末138側に出力する (s 1058)。一方、ユーザ権限が前記アクセス権限にマッチするものであれば (s 1057: Y)、前記更新リクエストに対応した更新処理を行い、この管理対象ファイルを暗号化し (s 1059)、前記ハードディスク115に保存する (s 1060)。

【0058】

サーバ100は、更新された管理対象ファイルの管理マスタ情報を抽出し、ファイル情報管理マスタデータベース110において該当ファイルの更新処理を行う (s 1061)。更新処理が完了した旨は、利用者端末138に送信され、利用者端末138ではこれを受信して表示する (s 1062)。

【0059】

図8は本実施形態の機密情報管理方法におけるファイル消去手順を示すフロー図である。本発明の機密情報管理方法においては、機密情報を含む管理対象ファイルを記憶装置たるハードディスク115より完全に消去する処理も可能とする。上記実施例では、委託側から受託者端末135が受託した管理対象ファイルについて、本発明の機密情報管理を適用している。従って、委託側との契約が終了したり、業務が完了したならば、関係する管理対象ファイルは消去する必要がある。

【0060】

ここで、関係する管理対象ファイルを消去する必要がある場合には、消去すべき管理対象ファイルを以下のようにして特定する。(1) 委託側と受託側の「業務委託契約書」に基づいて、管理対象ファイルを特定する。(2) 委託側と受託側で、消去が必要になった場合、情報を消去するための「消去契約書」を結び、これに基づいて、特定する。

【0061】

ここで、「業務委託契約書」および「消去契約書」を「契約書」と称する。「契約書」には、消去すべき管理対象ファイルを特定するための情報を列挙しておく。この特定するための情報としては、ファイル名、ファイル作成日時、ファイル使用時期、ファイル作成者の少なくとも1つを含む。この契約書が、紙で作成された場合、契約書に記載された「特定するための情報」を利用者が読み、委託者端末135 (もしくは管理者端末137) から消去対象の管理対象ファイルを入力する。これは、下記のステップs 1079のとおりである。

【0062】

次に、「契約書」が電子的に作成された場合、受託者端末135、委託側の端末もしくは管理サーバ100が、電子的な「契約書」の特定するための情報を読み取り、読み取られた場合、消去対象の管理対象ファイルの消去処理を開始する。

また、紙で契約書が作成された場合に、特定するための情報を電子的に作成しておき、電子的な契約書を作成した場合と同様の処理を実行してもよい。この特定するための情報は、受託情報管理マスタデータベース136に格納しておく。

また、さらに、電子的な契約書は、受託情報管理マスタデータベース136に格納しておいてもよい。

【0063】

なお、管理対象ファイルを消去する必要がある場合には、受託側から管理サーバ100に消去指示を送信してもよい。また、受託情報管理マスタデータベース136に、消去時期を格納しておいてもよい。この消去開始時期は、紙の契約書に基づいて、人手で入力してもよいし、電子的な契約書等に消去開始時期を含めておいてもよい。

【0064】

そこで、この時、受託者端末135では、消去対象の管理対象ファイルとその消去モードの選択(s1070)と、それら選択事象を含む消去リクエストの送信(s1071)がサーバ100に対して行われる。消去モードとは、管理対象ファイルのみを消去するモードと、管理対象ファイルのみならず、当該管理対象ファイルに対応するファイル情報管理マスタデータベース110における情報(管理マスタ情報)についても消去するモードとの二つが想定できる。

【0065】

サーバ100では前記の消去リクエストを受け付けて、この消去リクエストに対応する管理対象ファイルの情報をファイル情報管理マスタデータベース110より抽出する(s1072)。このとき、前記消去リクエストに対応する管理対象ファイルの情報に加えて、当該管理対象ファイルから派生した複製ファイルまたは更新ファイルの情報を、前記ファイル情報管理マスタデータベース110において抽出するものとする。

【0066】

サーバ100では、管理対象ファイルまたは複製ファイル或いは更新ファイルに関して抽出された情報に基づき、前記ハードディスク115またはバックアップ媒体116における該当ファイルの消去を実行する(s1073、s1074)。

【0067】

ここで、ハードディスク115(またはバックアップ媒体116)における消去処理の詳細について説明しておく。図9は本実施形態の機密情報管理方法におけるファイル消去手順詳細を示す概念図である。ここでいう詳細な処理とは、サーバ100は、消去対象のファイルがまだ残されている初期状態(s900)から、ハードディスク115における管理対象ファイルまたは複製ファイル或いは更新ファイルの消去を実行した後の状態(s901)に至り、開始される処理を指すものとする。

【0068】

この時、サーバ100は、ハードディスク115の格納情報、つまり消去されたファイル以外の残された全情報を、第2の記憶装置117にコピーする(s902)。また一方で、前記ハードディスク115におけるセクタなどの記憶単位毎に、所定パターンのデータを所定回書き込みして、ハードディスク115の全体消磁を実行する(s903)。

【0069】

続いて、前記第2の記憶装置117の格納情報(つまり消去対象のファイルが除かれたステップs901におけるハードディスク115の格納情報のコピー)を、前記ハードディスク115にコピーする(s904)。このコピーが完了したならば、前記第2の記憶装置117におけるセクタなどの記憶単位毎に、所定パターンのデータを所定回書き込んで、全体消磁を実行する(s905)。こうして消去処理は完了するのである(s906)。

【0070】

サーバ100は、上述のごとく消去された管理対象ファイルまたは複製ファイル或いは更新ファイルの、前記ファイル情報管理マスタデータベース110における該当管理マスタ情報の有効性の情報を、無効の旨に更新する(s1075)。消去リクエストに該当するファイルについての以上の処理が終了したかを判定し(s1076)、消去完了まで繰り返される(s1076:N~s1072~s1075)。一方、消去完了となった場合(s1076:Y)、前記消去モードの情報を抽出し、管理対象ファイルのみならず、当

該管理対象ファイルに対応するファイル情報管理マスタデータベース110における情報（管理マスタ情報）についても消去するモードか否かを判定する。ここで、前記消去リクエストに含まれる消去モード情報が、管理対象ファイルの消去に加えて管理マスタ情報の消去も要求するモードであった場合（s1077:Y）、前記ファイル情報管理マスタデータベース110における該管理対象ファイルの管理マスタ情報を特定し、消去する（s1078）。

【0071】

以上のようにして、消去リクエストに該当する管理対象ファイル等が消去されたならば、消去完了の旨を、受託者端末135に送信する（s1079）。受託者端末135ではこれを受信し、適宜な出力インターフェイス等に表示する（s1080）。また、受信した前記通知に基づき、消去された管理対象ファイル等の管理マスタ情報について、受託情報管理マスタデータベース136において該ファイルの更新処理を行う（s1081）。消去処理が完了した旨は、例えば印刷媒体に印刷され処理は終了する（s1082）。

【0072】

なお、上述した実施形態のように、機密情報管理方法の適用対象を管理対象ファイルとする例の他に、例えばこの管理対象ファイルを利用する業務アプリケーションのレベルで機密情報管理方法を適用する例も想定できる。この場合、前記業務アプリケーションの実行に際し、管理対象ファイルの消去権限、バックアップ権限、および利用権限のいずれかの有無をユーザ毎に定めた業務処理権限データベース111（図1参照）において、該ユーザの権限有無を判定するとともに、前記いずれかの権限をユーザが有する判定がなされた場合、業務アプリケーションの処理対象となる管理対象ファイルを前記ハードディスク115より抽出して、業務アプリケーションに提供するとする。

【0073】

本発明によれば、任意の情報の管理を効率よく実現できる。

【0074】

以上、本発明の実施の形態について、その実施の形態に基づき具体的に説明したが、これに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

【図面の簡単な説明】

【0075】

【図1】 本実施形態における情報処理装置を含むネットワーク構成図である。

【図2】 本実施形態における、（a）ファイル情報管理マスタデータベースのデータ構造例、（b）受託情報管理マスタデータベースのデータ構造例を示す図である。

【図3】 本実施形態におけるビジネスモデルの形態例である。

【図4】 本実施形態の機密情報管理方法におけるファイル登録手順を示すフロー図である。

【図5】 本実施形態の機密情報管理方法におけるファイル閲覧手順を示すフロー図である。

【図6】 本実施形態の機密情報管理方法におけるファイルバックアップ手順を示すフロー図である。

【図7】 本実施形態の機密情報管理方法におけるファイル更新手順を示すフロー図である。

【図8】 本実施形態の機密情報管理方法におけるファイル消去手順を示すフロー図である。

【図9】 本実施形態の機密情報管理方法におけるファイル消去手順詳細を示す概念図である。

【符号の説明】

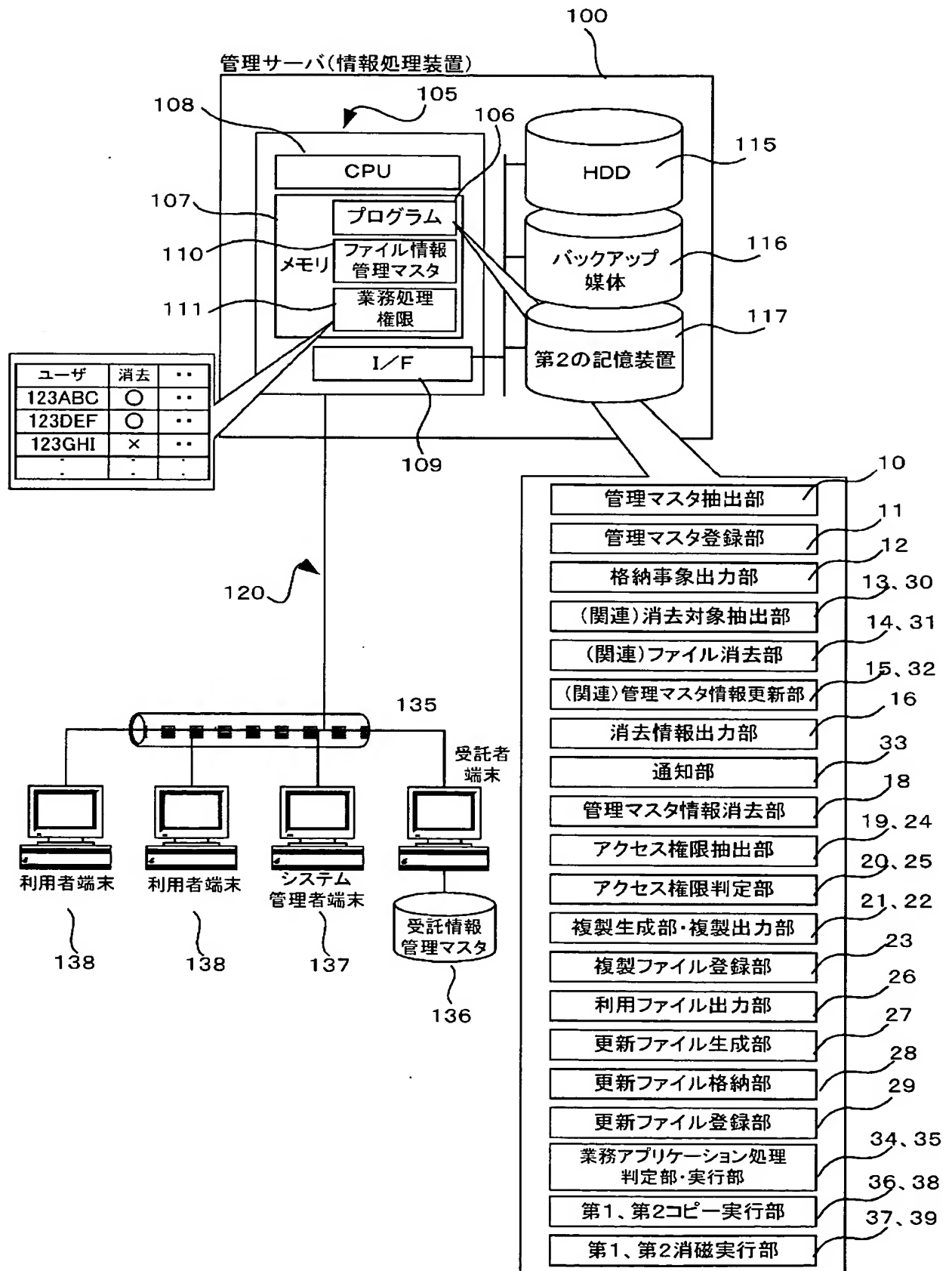
【0076】

- 10 管理マスタ抽出部
- 11 管理マスタ登録部
- 12 格納事象出力部

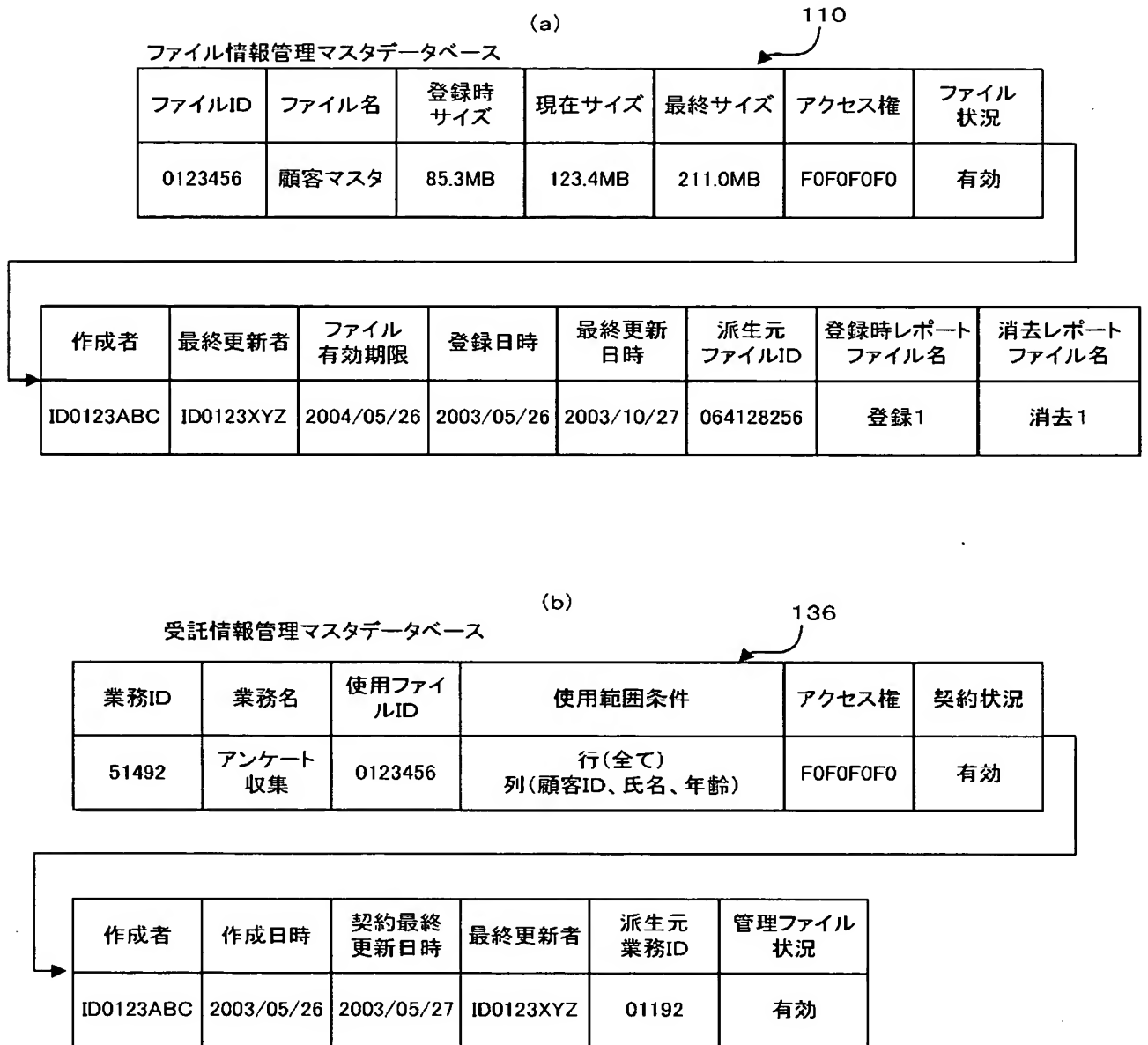
- 1 3 消去対象抽出部
- 1 4 ファイル消去部
- 1 5 管理マスタ情報更新部
- 1 6 消去情報出力部
- 1 0 0 管理サーバ（情報処理装置）
- 1 0 6 プログラム
- 1 0 7 メモリ
- 1 0 8 演算装置、C P U
- 1 0 9 入出力インターフェイス
- 1 1 0 ファイル情報管理マスタ（ファイル管理データベース）
- 1 1 1 業務処理権限データベース
- 1 1 5 ハードディスク（記憶装置）
- 1 1 6 バックアップ媒体
- 1 1 7 第 2 の記憶装置
- 1 2 0 ネットワーク
- 1 3 0 内部ネットワーク
- 1 3 5 受託者端末
- 1 3 6 受託情報管理マスタ
- 1 3 7 システム管理者端末
- 1 3 8 利用者端末

【書類名】 図面

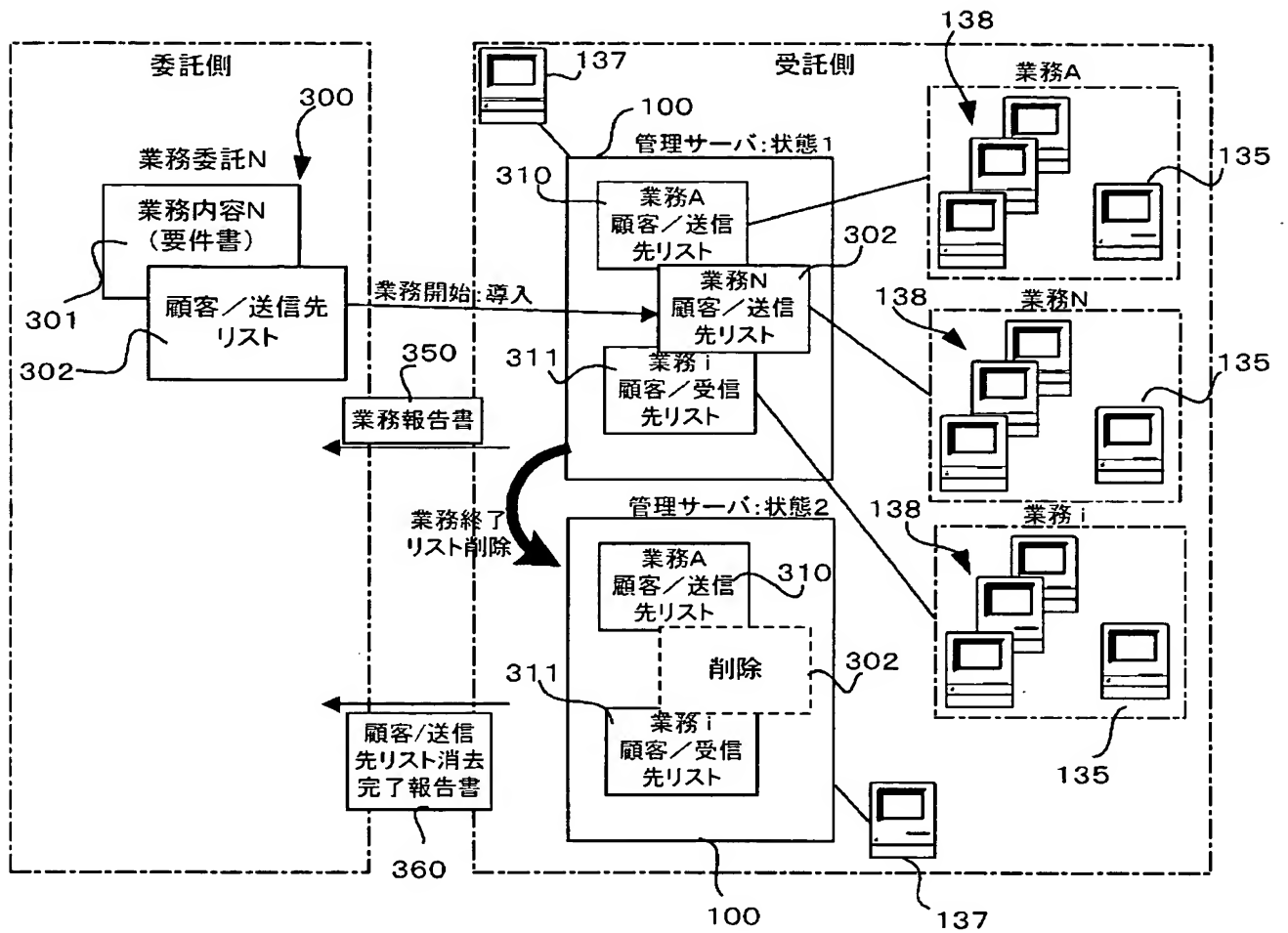
【図 1】



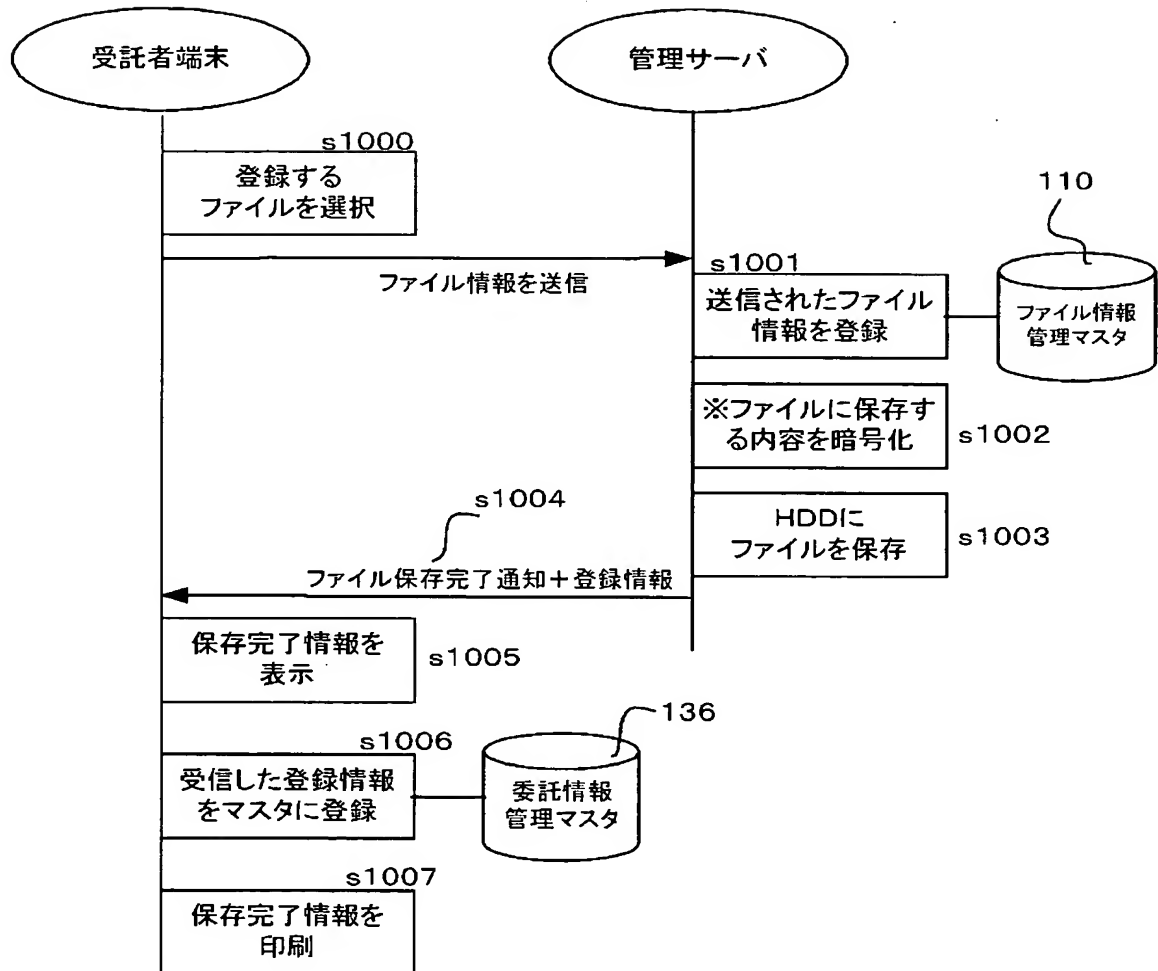
【図 2】



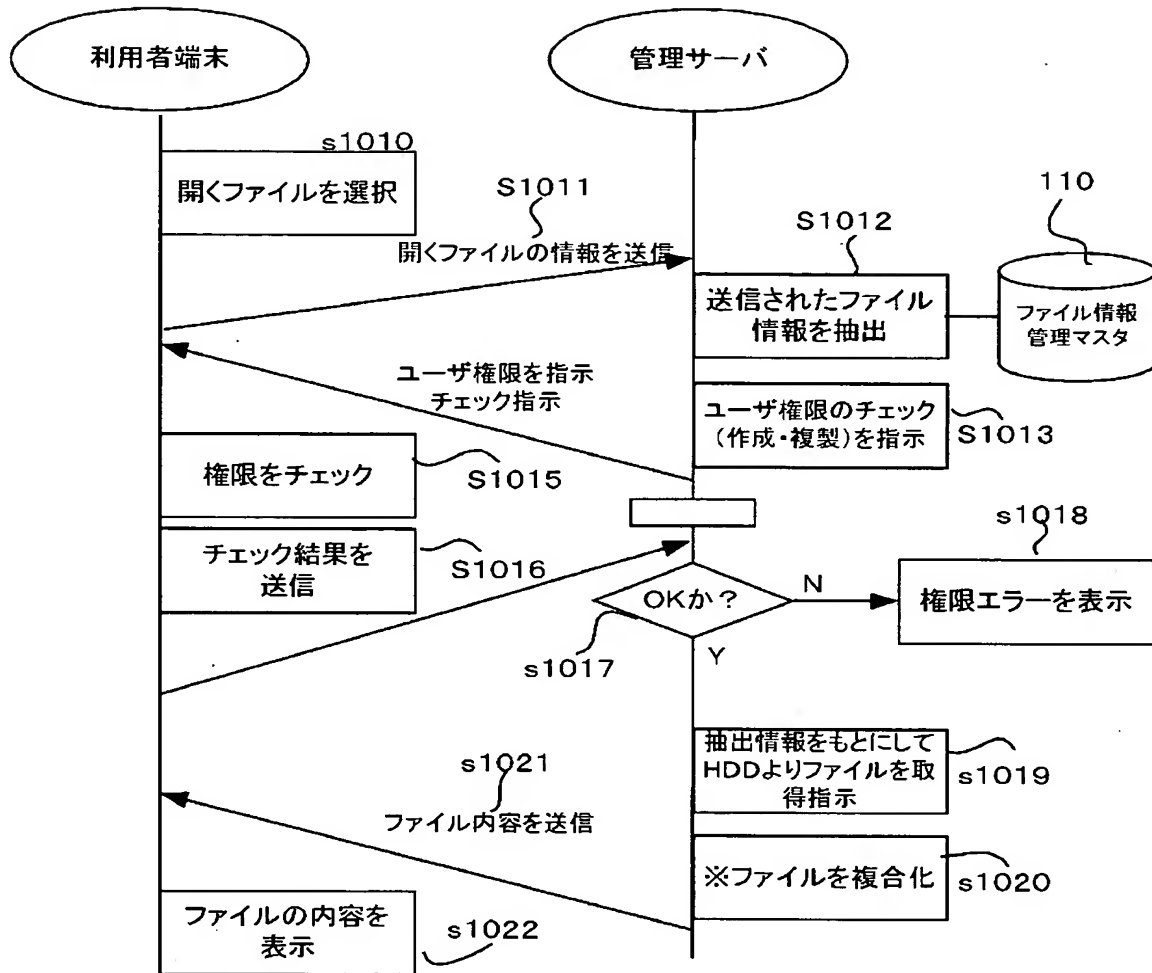
【図 3】



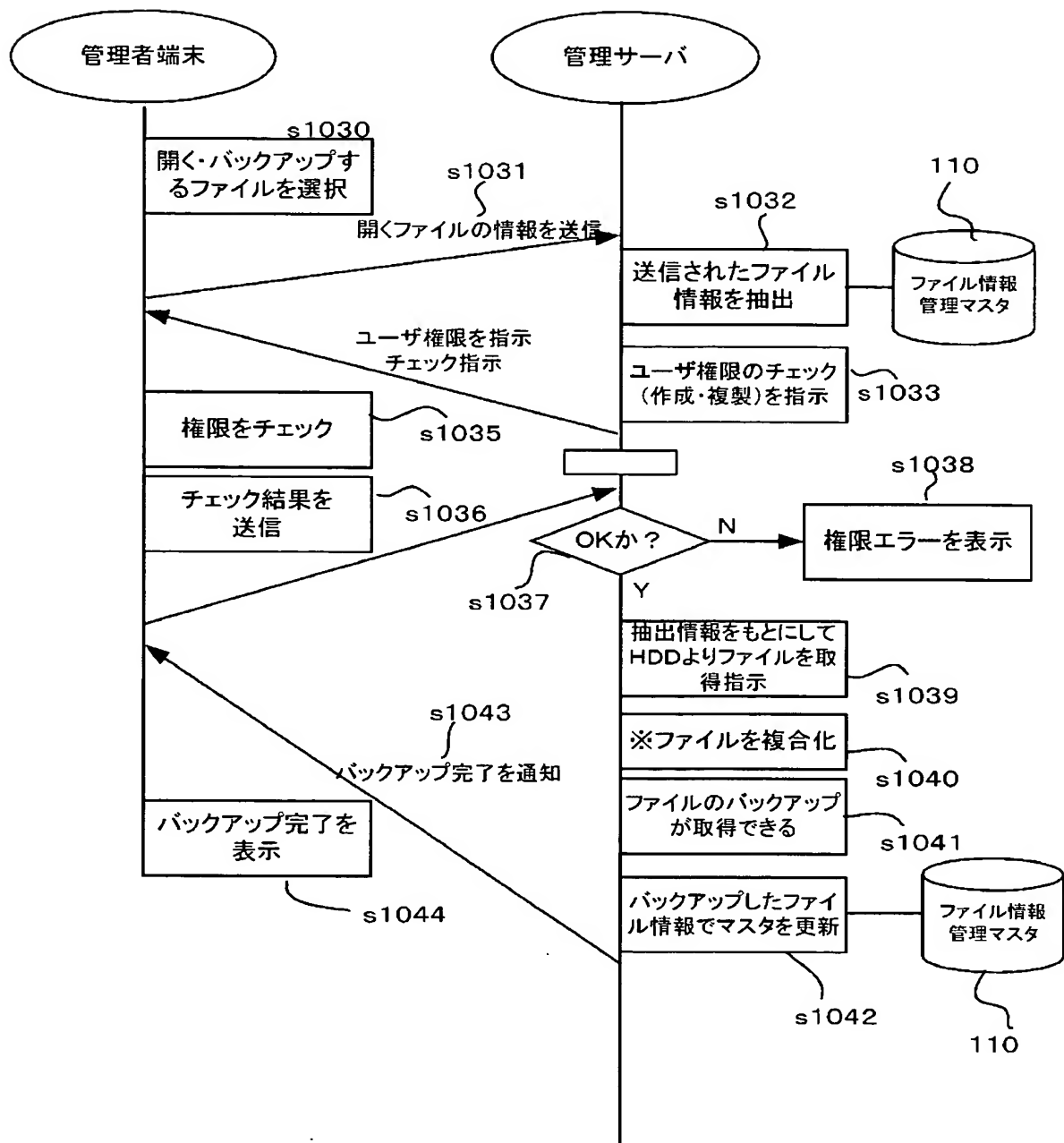
【図 4】



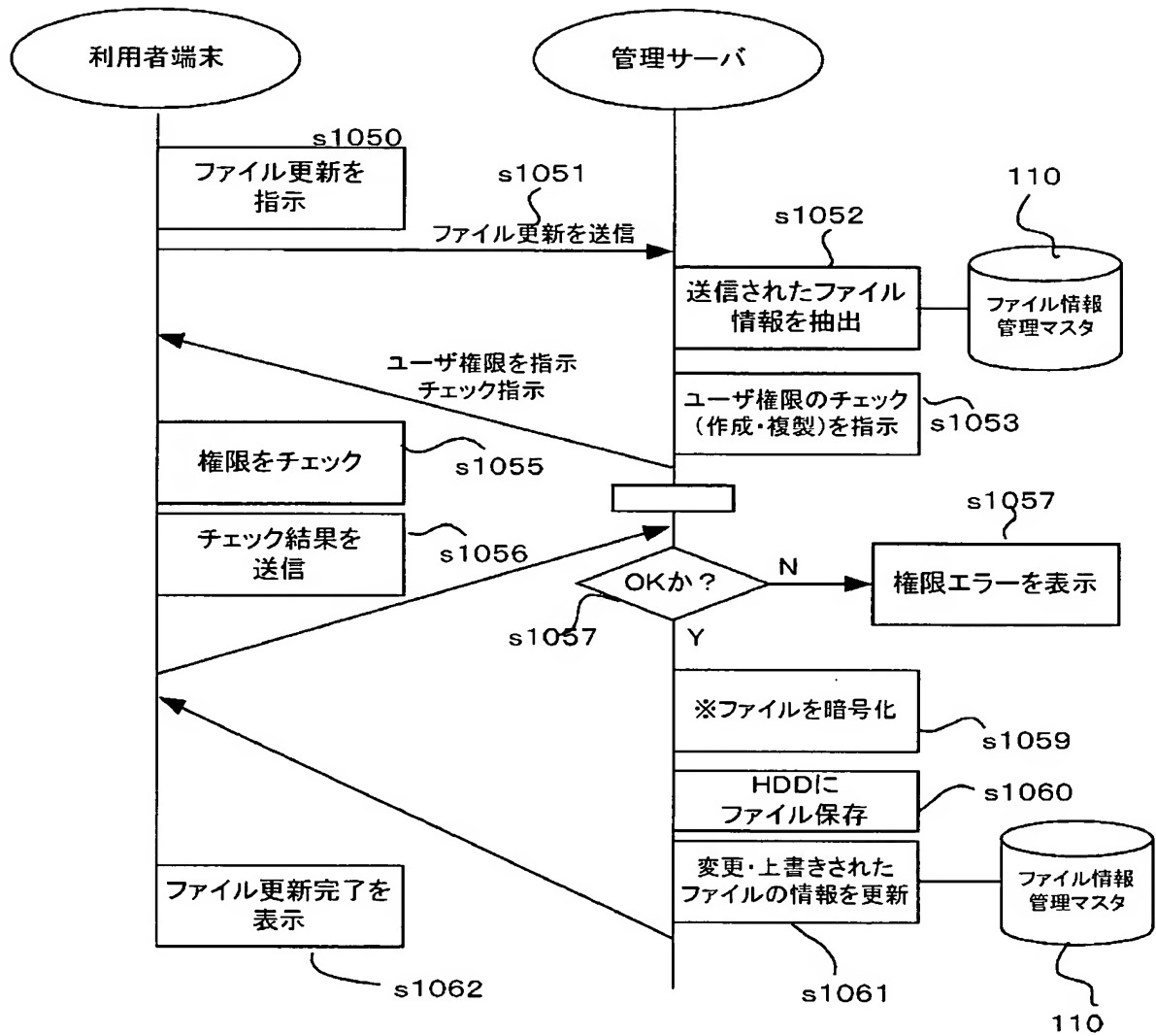
【図 5】



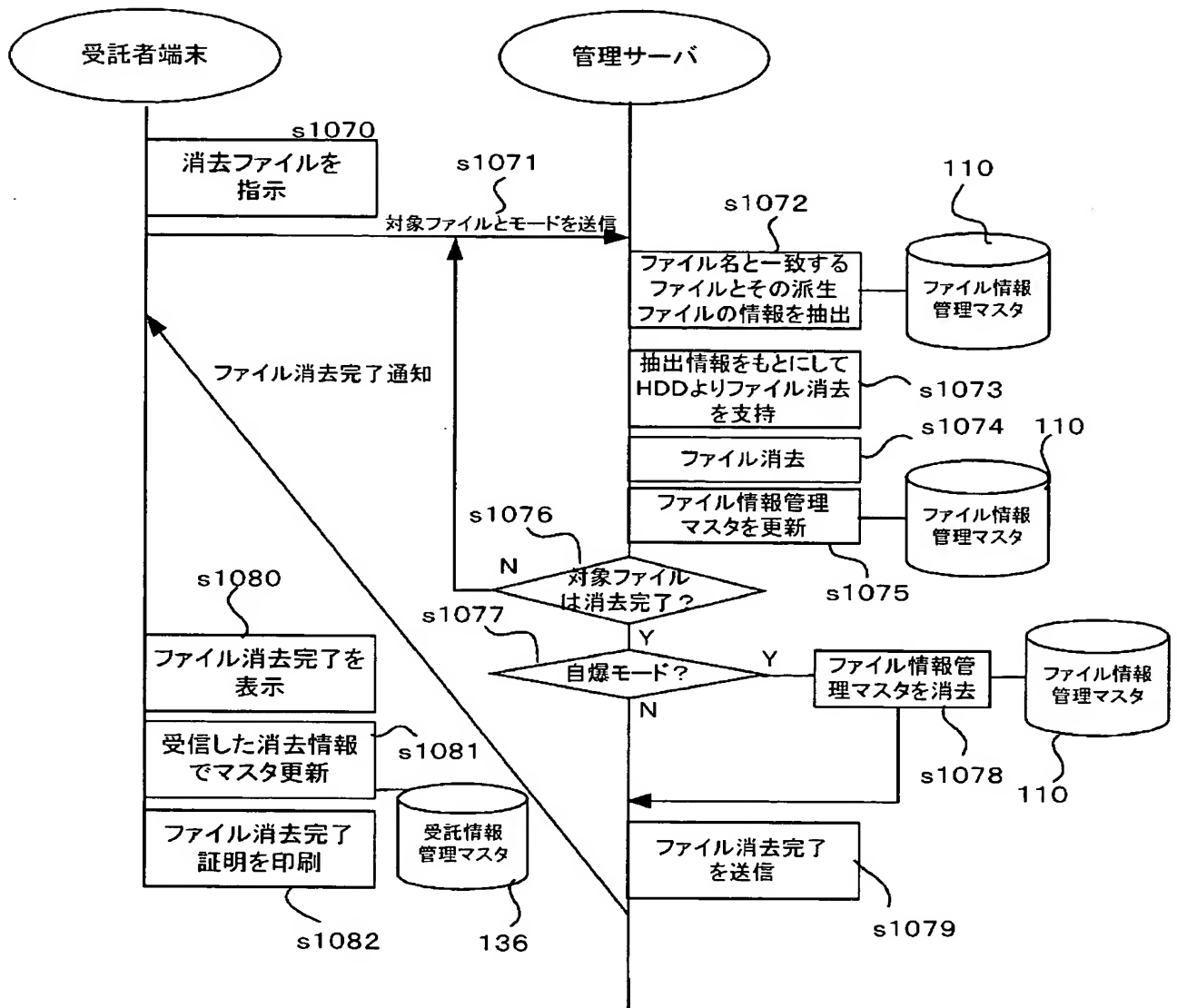
【図 6】



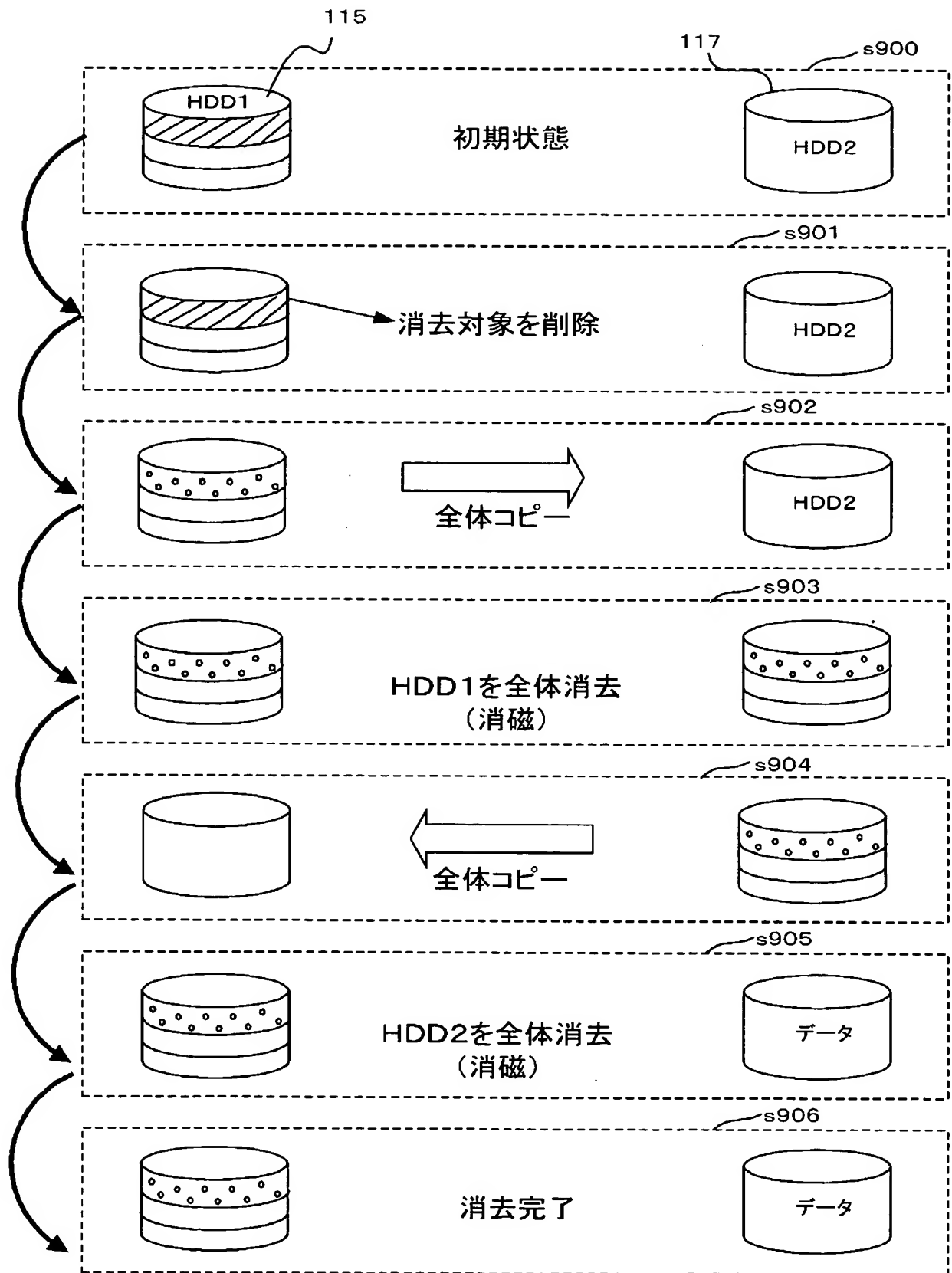
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 任意の情報の管理を効率よく実現する。

【解決手段】 管理対象ファイルより管理マスタ情報を抽出する管理マスタ抽出部 1 0 と、管理対象ファイル毎に前記管理マスタ情報が登録されたファイル管理データベースを格納する記憶装置 1 1 5 と、管理対象ファイルの記憶装置 1 1 5 への格納事象を出力する格納事象出力部 1 2 と、管理対象ファイルの消去リクエストに対応する管理対象ファイルの情報をファイル管理データベース 1 1 0 において抽出する消去対象抽出部 1 3 と、管理対象ファイルの情報に基づき記憶装置 1 1 5 における該当管理対象ファイルの消去を実行するファイル消去部 1 4 と、管理対象ファイルのファイル管理データベース 1 1 0 における該当管理マスタ情報の有効性の情報を無効の旨に更新する管理マスタ情報更新部 1 5 と、管理対象ファイルが消去された旨を出力する消去情報出力部 1 6 とを備える。

【選択図】 図 1

特願 2 0 0 3 - 3 8 2 5 8 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所